Semestre : 6

Unité d'enseignement : UED 3.2

Cours 2

Sécurité de l'information

Dr Mahmoud Hadef

Cryptographie

Partie 1 : Définition et Motivation

Partie 2: Le Chiffrement du Caesar

Partie 3 Le Chiffrement du Substitution

Partie 4 Le Chiffrement Poly-alphabétique

Références

- https://www.youtube.com/watch?v=hdomttjmsMg
- O. Paul ; Prévention des dénis de service dans les réseaux publics. Sécurité des systèmes d'information ; 2003.
- F. Raynal ; Canaux cachés. Sécurité des systèmes d'information ; 2003.
- T. Noel ; IP Mobile. Sécurité des systèmes d'information ; 2002.
- D. Trezentos ; Standard pour réseaux sans fil : IEEE 802.11. Sécurité des systèmes d'Informations ; 2002

Définition et Motivation

- La Cryptographie est la science de **transformation** de l'information pour qu'elle ne puisse pas être **ni lue ni comprise**.

- Notre objectif dans cette section est d'explorer comment cette science a pu de développer et prospérer bien que le cœur et le noyau de cette science sont la **sécurité** et la **confidentialité** ?

Définition et Motivation

- Aujourd'hui, cette science expose ses techniques, ses méthodes et ses algorithmes **publiquement**

- Elle les met sous l'analyse minutieux et méticuleux des programmeurs et hackeurs du **monde entier**.

- Mais ça n'a pas toujours était le cas, pour des siècles et des siècles beaucoup d'efforts ont été investi pour **sécuriser la méthode de sécurisation** de communication.

Système du Chiffrement

Dans la cryptographie a clé publique, la clé du Chiffrement est connue

Clé du Chiffrement

Donc, dans la cryptographie a clé publique, la seule clé qui est secrète est la clé du déchiffrement

Clé du Déchiffrement

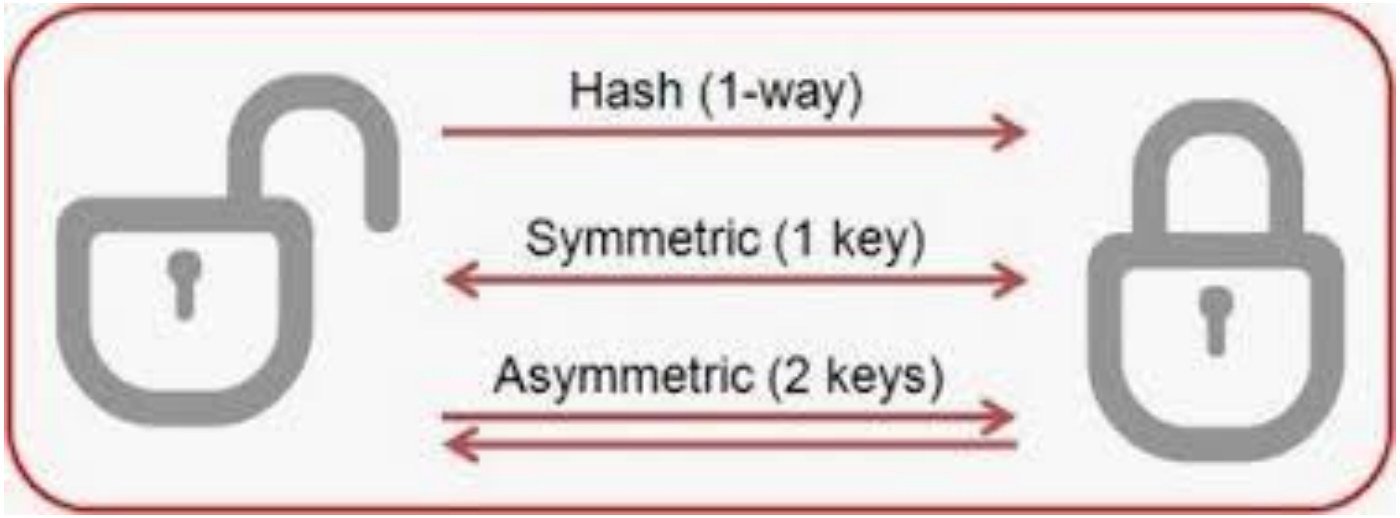
Message → Algorithme du Chiffrement → Cryptogramme → Algorithme du Déchiffrement → Message

Source

Destinataire

Dans la cryptographie a clé publique :
Les algorithmes du chiffrement et déchiffrement sont connus

Types de Cryptographie



- Système du **chiffrement symétrique** conventionnel ou il est facile de déduire la clé du déchiffrement a partir de la clé du chiffrement.

Types de Cryptographie

- Pour la plupart des chiffrements symétriques, les clés du chiffrement et du déchiffrement **sont les mêmes,** elles sont souvent nommées **les clés secrètes.**

- Dans un système du **chiffrement asymétrique,** il est impossible de déduire la clé du déchiffrement a partir de la clé du chiffrement.

Les Pires des Cas

- Le cryptanalyste a un savoir complet du système du chiffrement

Le système du chiffrement sera connu partiellement ou totalement

(Exemple: l'analyste polonais a connu la structure du hardware qui constituait le cœur **de l'Enigme**).

Marian Rejewski

Les Pires des Cas

- Le cryptanalyste a obtenu une quantité considérable du texte chiffré: une supposition raisonnable, sinon pourquoi on chiffre, si on est certain que personne ne verra notre message?

- Le cryptanalyste connait l'équivalent en texte d'une certaine partie du texte chiffré: par exemple en connaissant que le texte est une lettre et que la structure générale d'une lettre commence par «cher»,

Chiffrement du Caesar

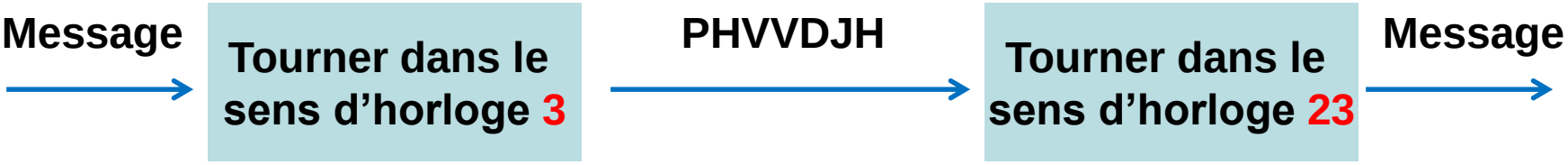
- Ecrire les **26** lettres au tour du cercle extérieur.
- Chaque lettre de l'alphabet est décalée **13** fois dans le sens de l'horloge, cette deuxième alphabet décalée forme le cercle intérieur.
- *Exemple*: le mot «**Guerre**» devient «**Threer**»

Chiffrement du Caesar: Exemple

Dans ce cas les clés sont différentes mais les algorithmes sont les mêmes. Si on veut garder la même clé de chiffrement et du déchiffrement: 3, il faudrait donc changer l'algorithme du déchiffrement qui devient: tourner dans le sens contraire d'horloge 3 fois

Clé du Chiffrement: 3

Clé du déchiffrement: 23



Le Désavantage de Chiffrement de Caesar

Enciphering key	Possible message	Enciphering key	Possible message	Enciphering key	Possible message
0	AFCCP	17	JOLLY	8	SXUUH
25	BGDDQ	16	KPMMZ	7	TYVVI
24	CHEER	15	LQNNA	6	UZWWJ
23	DIFFS	14	MROOB	5	VAXXK
22	EJGGT	13	NSPPC	4	WBYYL
21	FKHHU	12	OTQQD	3	XCZZM
20	GLIIV	11	PURRE	2	YDAAN
19	HMJJW	10	QVSSF	1	ZEBBO
18	INKKX	9	RWTTG		

Le Désavantage de Chiffrement de Caesar

- Le cryptogramme: **AFCCP:** Dans cet exemple, deux clés seulement résultent en des mots compréhensibles en Anglais, donc déjà on a éliminé **26** clés, et avec un peu plus de texte, on pourrait éliminer une autre clé, et on aura la clé finale.

- Le chiffrement de Caesar est très vulnérable aux **attaques de force brute**, c'est-à-dire, la recherche exhaustive des clés, car il y'a seulement **26** clés a essayer.

Les Chiffrements du Substitution

- Ecrire l'alphabet dans l'ordre alphabétique.
- Ecrire l'alphabet en un ordre aléatoire sous l'alphabet. *Exemple*:

A B C D E F G H I J K L M O N P Q R S T U V W X Y Z

P H Q G I U M E A Y L N O F D X J K R C V S T Z W B

- Les clés de chiffrement et déchiffrement sont les mêmes et dans ce cas, l'ordre de l'alphabet rouge.
- L'algorithme du chiffrement est de remplacer chaque lettre avec la lettre en dessous.
- L'algorithme du déchiffrement est de remplacer chaque lettre avec la lettre en dessus.

Les Chiffrements du Substitution

- Nombre de clés possible = 26 * 25 * 24 * 23…..*3*2*1

  = **403, 291, 461, 126, 605, 635, 584,000, 000**
- Même si on essaie 1 billion clés / seconde → 13 billions années pour essayer toutes les clés.
- Le problème avec ces clés est qu'elles sont très difficiles a mémoriser.
- Donc il y'a une tendance a mémoriser les clés a travers une phrase mnémonique.

Le Désavantage du Chiffrement du Substitution

E	11.1607%	56.88	M	3.0129%	15.36
A	8.4966%	43.31	H	3.0034%	15.31
R	7.5809%	38.64	G	2.4705%	12.59
I	7.5448%	38.45	B	2.0720%	10.56
O	7.1635%	36.51	F	1.8121%	9.24
T	6.9509%	35.43	Y	1.7779%	9.06
N	6.6544%	33.92	W	1.2899%	6.57
S	5.7351%	29.23	K	1.1016%	5.61
L	5.4893%	27.98	V	1.0074%	5.13
C	4.5388%	23.13	X	0.2902%	1.48
U	3.6308%	18.51	Z	0.2722%	1.39
D	3.3844%	17.25	J	0.1965%	1.00
P	3.1671%	16.14	Q	0.1962%	(1)

Le Désavantage du Chiffrement du Substitution

- Puisque on peut extraire l'analyse de fréquence de chaque lettre en n'importe quel langue, donc on peut conclure l'equivalent d'une lettre chiffrée a partir de sa fréquence.
- Exemple: si on substitue la lettre « **E**» avec la lettre «**W**», et puis on prend le texte chiffré en on applique l'analyse de fréquence, on y trouvera que la fréquence de la lettre «**W**» est approximativement **11.16%** donc on peut facilement conclure que la lettre «**W**» est la substituée de la lettre «**E**»

Le Chiffrement du Vigenere

Texte

AGEDTWENTYSIX
VIGENERE

Clé

CHARLESVCHARL
ESV

Texte Chiffré

CNEUEAWIVFSZIZ
ABGUEIP